February 20, 2019

Via Electronic Comment Filing System
Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, Suite CY-B402
Washington, DC 20554

RE: AST Telecom, LLC.
CPNI Certification
EB Docket No. 06-36

Dear Ms. Dortch:

On behalf of AST Telecom, LLC dba Bluesky Communications, pursuant to 47 C.F.R. § 64.2009(e), enclosed is its Customer Proprietary Network Information ("CPNI") certification for 2019 covering the prior calendar year 2018.

Sincerely,

Raj Deo

Attachment
CC: Best Copy and Printing Inc. (via-email)

Annual 47 C.F.R § 64.2009(e) CPNI Certification
EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering calendar year 2018

1. Date filed: February 20, 2019
2. Name of company covered by this certification:

AST Telecom, LLC d/b/a Bluesky Communications

3. Form 499 Filer ID: **831587**
4. Name of Signatory: **Raj Deo**
5. Title of Signatory **Country Manager**
6. Certification:

I, Raj Deo, hereby certify that I am an officer of the Company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules set forth in 47 C.F.R. §§64.2001 *et seq.* of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has received one complaint in the past year concerning unauthorized release of CPNI. The complaint was a result of unauthorized disclosure of call records information to customers spouse.

The company represents and warrants that the above certification is consistent with 47 C.F.R § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Raj Deo

Attachment: Accompanying Statement explaining CPNI procedures

AST Telecom, LLC d/b/a Bluesky Communications
Attachment

STATEMENT

Pursuant to Section § 64.2009€ of the Federal Communications Commission's rules, this statement explains how AST Telecom, LLC d/b/a Bluesky Communications' (the "Company") operating procedures ensure compliance with Part 64, Subpart U, of the FCC 's rules.

Company's Usage of CPNI

- The Company has chosen to prohibit the use of CPNI for marketing purposes by itself and between affiliates.
- The Company has CPNI procedures that set forth the Company's CPNI policies and outline what CPNI is and when it may or may not be used without customer approval by the Company.
- The Company's Procedures provide that the Company may use CPNI to protect its rights and property, customers, and other carriers form fraudulent, abusive or unlawful use of, or subscription to, the Company's services.
- The Company's Procedures require the affirmative written/electronic customer approval for the release of CPNI to third parties.

Company's CPNI Safeguards

- The Company has established procedures for the training of its personnel with access to customer CPNI. Employees have been trained as to when they are and are not authorized to use CPNI. The Company's CPNI Procedures describe the disciplinary process related to noncompliance with CPNI obligations. Refresher training courses are often scheduled.
- The Company's CPNI Procedures and/or employees manuals contain express disciplinary procedures applicable to employees who violate Company policies, including CPNI policies, which can include termination of employment.
- The Company has established a supervisory review process regarding Company Compliance with the FCC's CPNI rules. The Company's CPNI Certifying officer is held responsible for annually certifying that the Company is in compliance with the FCC's CPNI rules and submitting such certification and accompanying statement of how the company complies with the FCC's CPNI rules to the FCC by March 1st of every year.
- The Company takes reasonable measure to discover and protect against attempts to gain unauthorized access to CPNI. The Company authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact or an in-store-visit.
- The Company only discloses call detail information over the telephone, based on customer initiated telephone contact, if the customer first provides a password that

is not prompted by the carrier asking for readily available biographical information or account information. If a customer does not provide a password, the Company only discloses call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the customer is able to provide call detail information during a customer initiated call without the Company's assistance, then the Company is permitted to discuss the call detail information provided by the customer.

- The Company has established a system of passwords and password protection. For a new customer (a customer that establishes services after the effective date of the new CPNI rules) the Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, the customer must visit the Company's retail store at which time the retail representative must establish that the person at the counter is indeed the registered person whose name is on the account by valid photograph identifications such as a Passport, Government ID, Driver's License and/or Immigration ID.

- For accounts that are password-protected, the Company cannot obtain the password by asking for readily available biographical information or account information to prompt the customer for his/her password. If a password is forgotten or lost, the Company uses a backup customer authentication method that is not based on readily available biographical information or account information.

- If a customer is able to provide to the Company, during the customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e. the telephone number called, when it was called, and if applicable, the amount charged for the call) then the Company proceeds with its routine customer carrier procedures. Under these circumstances, the Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.

- The Company may provide customers with access to CPNI at a carrier's retail location if the customer presents a valid photo ID and the valid photo ID matches the name of the account. The Company, at this time, does not provide online access for customers.

- The Company notifies a customer immediately when a password, customer response to a backup means of authentication for lost or forgotten passwords, or address of record is created or changed by mail to the address of record.

- In the event of a CPNI breach, the Company delays customer notification of breaches until the law enforcement has been notified of a CPNI breach. The Company will notify law enforcement of a breach of its customers' CPNI within seven (7) business days after making a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the FBI. If the relevant investigating agency determines that public disclosure of notice to customers would impede or compromise an ongoing or potential criminal investigation for national security, that agency may direct the Company not to disclose the breach for an initial 30-day period. The law enforcement

agency must provide in writing to the carrier it is initial direction and any subsequent direction.

- The Company, however, may immediately notify a customer or disclose the breach publicly after the consultation with the relevant investigative agency, if the Company believes there is any extraordinarily urgent need to notify a customer or class of customers to avoid immediate and irreparable harm.

- The Company maintains a record of any discovered breaches and notification to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notification for a period of at least two years.

- The following is a summary of all customer complaints received in 2018 regarding unauthorized release of CPNI:

  - Number of customer complaints Carrier received in 2018 related to unauthorized access to CPNI, or unauthorized disclosure of CPNI: 1

  - Category of Complaint:

    0 Number of instances of improper access by employees

    1 Number of instances of improper disclosure to individuals not authorized to receive information

    0 Number of instances of improper access to online information by individuals not authorized to view the information

    0 Number of other instances of improper access or disclosure

  - Summary of customer complaints received in 2018 concerning the unauthorized release of CPNI: 1